係数ドメインを多項式環とする多項式環の簡約グレブナ基底について (Computer Algebra : Design of Algorithms, Implementations and Applications)

AUTHOR(S):

鍋島, 克輔

数理解析研究所講究録
第1652巻 2009年 1-10

係数ドメインを多項式環とする多項式環の簡約グレブナ基底について

鍋島克輔
科学技術振興機構 (JST) / 東京大学・情報理工学系研究科*
NABESHIMA, KATSUSUKE
Japan Science and Technology Agency (JST)/
Graduate School of Information Science and Technology,
The University of Tokyo

1 はじめに

グレブナ基底の有用性はさまざまな分野で広く知られており，多くの研究者によってさまざまなドメイン上でのグレブナ基底が研究されている。例えば，係数ドメインを Euclid 整域 [KRK88]，整数環 [NG94]，可換な正規環 [Wei87]，Noether 環 [Tri78, AL94]，リダクション環 [Sti87] などとした多項式環上でもグレブナ基底は定義され，それぞれのドメインで研究されている。本論文では，係数ドメインを多項式環とする多項式環上での簡約グレブナ基底とそれを求めるアルゴリズムについて考察する。ここで，K を体とし $\bar{X}$, $\bar{A}$ を $\bar{X} \cap \bar{A} = \emptyset$ となる変数の集合とする。このとき，$K[\bar{A}][\bar{X}]$(係数ドメインを多項式環とする多項式環) 上でのグレブナ基底の計算方法としてよく知られたものは，ブロック項順序 $\bar{X} \gg \bar{A}$ をもちいて $K[\bar{A}, \bar{X}]$ 上でグレブナ基底を計算することである。しかしながら，この方法だと冗長な多項式がよく現れ簡約グレブナ基底を計算することはできない。他に syzygy を使ったグレブナ基底計算方法が存在する。しかしながら，この場合にも問題があり簡約グレブナ基底を計算することはできない。本論文では，これらの問題を紹介するとともに簡約グレブナ基底を新しく定義し，それを求めるアルゴリズムを与える。また，全てのイデアルは唯一な簡約グレブナ基底を持つことを示す。

2 記号

本稿において以下の記号を固定する。K を体とし L を K の拡大体とする。$\bar{X} = \{X_1, \ldots, X_n\}$, $\bar{A} = \{A_1, \ldots, A_m\}$ を変数とし $\bar{X} \cap \bar{A} = \emptyset$ とする。$\mathrm{pp}(\bar{X})$, $\mathrm{pp}(\bar{A})$, $\mathrm{pp}(\bar{A}, \bar{X})$ を順に $\bar{X}$ の項 (power product) の集合，$\bar{A}$ の項の集合，$\bar{X} \cup \bar{A}$ の項の集合とする。$\mathbb{N}$ を自然数の集合 (0 を含む)，$\mathbb{Q}$ を有理数体，$\mathbb{C}$ を複素数体とする。$K[\bar{A}][\bar{X}] := (K[\bar{A}])[\bar{X}]$ を多項式環 $K[\bar{A}]$ を係数ドメインとする多項式環とする。いま， 多項式 f を 0 でない $K[\bar{A}, \bar{X}]$ (または $K[\bar{A}][\bar{X}]$) の元とする。ここで $\mathrm{pp}(\bar{A}, \bar{X})$ (または $\mathrm{pp}(\bar{X})$) 上の任意の項順序を $\succ$ としたとき以下を定義する。(もし，f が $K[\bar{A}][\bar{X}]$ の元のとき $K[\bar{A}, \bar{X}]$ の元との混乱をさせるため添え字 $\bar{X}$ を付ける。) f の**先頭項**を $\mathrm{lpp}(f)$ (または $\mathrm{lpp}_{\bar{X}}(f)$) (leading power product)，**先頭係数**を $\mathrm{lc}(f)$ (または $\mathrm{lc}_{\bar{X}}(f)$) (leading coefficient)，**先頭単項**を $\mathrm{lm}(f) := \mathrm{lc}(f)\,\mathrm{lm}(f)$ (または $\mathrm{lm}_{\bar{X}}(f)$) (leading monomial) と書く。多

*Katsusuke_Nabeshima@ipc.i.u-tokyo.ac.jp

項式 f の**単項の集合**を $\mathrm{Mono}(f)$ (または $\mathrm{Mono}_{\bar{X}}(f)$) と書く。もし，$\mathrm{lpp}(f) = A_1^{\alpha_1}\cdots A_m^{\alpha_m}X_1^{\beta_1}\cdots X_n^{\beta_n} \in \mathrm{pp}(\bar{A},\bar{X})$ なら**次数**として $\deg_{\{\bar{A},\bar{X}\}}(f) := (\alpha_1,\ldots,\alpha_m,\beta_1,\ldots,\beta_n) \in \mathbb{N}^{m+n}$，$\deg_{X_1}(f) := \beta_1 \in \mathbb{N}$ と表す。F を $K[\bar{A},\bar{X}]$ (または $K[\bar{A}][\bar{X}]$) の多項式の集合とする。そのとき，$\mathrm{lc}(F) := \{\mathrm{lc}(f) : f \in F\}$ (または $\mathrm{lc}_{\bar{X}}(F) := \{\mathrm{lc}_{\bar{X}}(f) : f \in F\}$), $\mathrm{lpp}(f) := \{\mathrm{lpp}(f) : f \in F\}$ (または $\mathrm{lpp}_{\bar{X}}(F) := \{\mathrm{lpp}_{\bar{X}}(f) : f \in F\}$) とする。

例 1
a,b,x,y を変数とし，$f = 2ax^2y + bx^2y + 3x + by + 1$ を多項式とする。もし f を $\mathbb{Q}[x,y,a,b]$ の元と見ると，辞書式順序 $x \succ y \succ a \succ y$ に関して以下となる。$\mathrm{lpp}(f) = ax^2y$, $\mathrm{lc}(f) = 2$, $\mathrm{lm}(f) = 2ax^2y$, $\mathrm{Mono}(f) = \{2ax^2y, bx^2y, 3x, by, 1\}$。次に，$f$ を $\mathbb{Q}[a,b][x,y]$ の元と見ると，辞書式順序 $x \succ y$ に関して，以下となる。$\mathrm{lpp}_{\{x,y\}}(f) = x^2y$, $\mathrm{lc}_{\{x,y\}}(f) = 2a+b$, $\mathrm{lm}_{\{x,y\}}(f) = (2a+b)x^2y$, $\mathrm{Mono}_{\{x,y\}}(f) = \{(2a+b)x^2y, 3x, by, 1\}$。

本稿では $\mathbb{V}$ と三角カッコ (angle brackets) $\langle\ \cdot\ \rangle$ を次のように定義する。$f_1,\ldots,f_l \in K[\bar{A}]$ において，$\mathbb{V}(f_1,\ldots,f_l) \subset L^m$ を $f_1,\ldots,f_l$ のアフェイン代数多様体と定義する。すなわち，$\mathbb{V}(f_1,\ldots,f_k) = \{\bar{a} \in L^m : f_1(\bar{a}) = \cdots = f_k(\bar{a}) = 0\}$。$R$ を単位元を持つ可換環とする。 そのとき，$f_1,\ldots,f_l \in R$ において $\langle f_1,\ldots,f_l\rangle := \{\sum_{i=1}^{s} h_i f_i : h_1,\ldots,h_s \in R\}$ とする。

定義 1 (ブロック項順序)
$\mathrm{pp}(\bar{A})$ 上の項順序を $\succ_1$，$\mathrm{pp}(\bar{A})$ 上の項順序を $\succ_2$ とし，$t_1,s_1 \in \mathrm{pp}(\bar{A})$, $t_2,s_2 \in \mathrm{pp}(\bar{X})$ とする。その時，$\mathrm{pp}(\bar{A},\bar{X})$ 上の項順序 $\succ_{\bar{X},\bar{A}}$ を次のように定義する。

$$t_1t_2 \succ_{\bar{X},\bar{A}} s_1s_2 \iff t_2 \succ_2 s_2 \text{ or } (t_2 = s_2, \text{ and } t_1 \succ_1 s_1)$$

この項順序 $\succ_{\bar{X},\bar{A}}$ を $\mathrm{pp}(\bar{A},\bar{X})$ 上の**ブロック項順序 (block order)** と言い，$\succ_{\bar{X},\bar{A}} = (\succ_2,\succ_1)$ と書く。

3 計算法と問題点

ここでは $K[\bar{A}][\bar{X}]$ 上の多項式イデアルのグレブナ基底を計算するために 2 つの知られた計算方法を見る。

3.1 第 1 の計算方法

まず，特別な S-多項式とリダクションを使った $K[\bar{A}][\bar{X}]$ 上のグレブナ基底の計算法を紹介する。[IP98, AL94, Möl88]

定義 2 (リダクション [AL94])
2 つの多項式 f,h とゼロでない多項式の集合 $F = \{f_1,\ldots,f_s\} \subset K[\bar{A}][\bar{X}]$ が与えれたとき，f は F によって h へ**リダクション (reducetion)** されるとは，$\mathrm{lc}_{\bar{X}}(f) = c_1\,\mathrm{lc}_{\bar{X}}(f_1) + \cdots + c_s\,\mathrm{lc}_{\bar{X}}(f_s)$ となる $c_1,\ldots,c_s \in K[\bar{A}]$ と $\mathrm{lpp}_{\bar{X}}(f) = D_i\,\mathrm{lpp}_{\bar{X}}(f_i)$ となる $D_1,\ldots,D_s$ が存在するとき，$h = f - (c_1D_1f_1 + \cdots + c_sD_sf_s)$ となる。

定義 3 (S-多項式 [AL94, IP98])
G を $K[\bar{A}][\bar{X}]$ の有限集合，I を G で生成された $K[\bar{A}][\bar{X}]$ のイデアルとし，各 $E \subseteq G$ において，$S_E := \{(c_e)_{e\in E} | \sum_{e\in E} c_e\,\mathrm{lc}_{\bar{X}}(e) = 0\}$ とする。その時，各 $s = (c_e)_{e\in E} \in S_E$ において，
$\mathrm{Spoly1}(E,s) = \sum_{e\in E} c_eX^{\max(E)-\deg_{\bar{X}}(e)}e$ を s に関する **S-多項式 (S-polynomial)** と言う。ここで，$\max(E) := (\max_{e\in E}\deg_{\bar{X}}(e)_1,\ldots,\max_{e\in E}\deg_{\bar{X}}(e)_n) \in \mathbb{N}^n$ とする。本論文において，この特別な S-多項式を "Spoly1" と書く。実際，S_E は有限な $\mathrm{lc}_{\bar{X}}(E)$ の syzygy 加群の生成元の集合である。

$K[\bar{A}][\bar{X}]$ 上でのグレブナ基底の定義は以下である。

定義 4 (グレブナ基底)
$\mathrm{pp}(\bar{X})$ 上の項順序を $\succ$ と固定する。もし，イデアル $I \subseteq K[\bar{A}][\bar{X}]$ の有限部分集合 $G = \{g_1, \ldots, g_s\}$ が $\langle \mathrm{lm}_{\bar{X}}(g_1), \ldots, \mathrm{lm}_{\bar{X}}(g_s) \rangle = \langle \mathrm{lm}_{\bar{X}}(I) \rangle$ を満たすとき G を $\succ$ に関して I の**グレブナ基底 (Gröbner basis)** と言う。
注意: この定義は次と同値である。
各 $i \in \mathbb{N}^n$ において，$\mathrm{lc}(i, I) := \langle \mathrm{lc}_{\bar{X}}(f) | f \in I, \deg_{\bar{X}}(f) = i \rangle$ とする。その時，各 $i \in \mathbb{N}^n$ で，イデアル $\mathrm{lc}(i, I) \subseteq K[\bar{A}]$ が $\{ \mathrm{lc}_{\bar{X}}(g) \mid g \in G, i \in \deg_{\bar{X}}(g) + \mathbb{N}^n \}$ によって生成されるなら G は I の ($\succ$ に関する) グレブナ基底と言う。

体を係数ドメインとする一般的なグレブナ基底と同様に $K[\bar{A}][\bar{X}]$ 上のグレブナ基底にも多くの良い性質，応用がある。しかしながら，本論文ではそれは述べない。参照 [IP98, AL94]。

アルゴリズム 1 FirstGB($F, \succ$)
Input: F: $K[\bar{A}][\bar{X}]$ の有限部分集合，$\succ$: $\mathrm{pp}(\bar{X})$ の項順序，
Output: G: $\succ$ に関する $\langle F \rangle$ のグレブナ基底。
• ブッフバーガー (Buchberger)[Buc65] のグレブナ基底計算アルゴリズムのように，これらの特別な S-多項式とリダクションを使ってアルゴリズムを構成することができる。参照 [AL94, Chapter 4]。

このアルゴリズムにより，$K[\bar{A}][\bar{X}]$ 上のイデアルのグレブナ基底の計算ができる。しかしながら，この計算方法は次のような問題がある。

問題 1
$\mathbb{Q}[a][x]$ 上の多項式 $f_1 = a^2x - a$ と $f_2 = (a^3 - a)x - a^2 + 1$ を考える。この 2 つから生成されるイデアルのグレブナ基底は，リダクションと S-多項式よる $f_1 \xrightarrow{f_2}_{r1} f_1$，$f_2 \xrightarrow{f_1}_{r1} f_2$，S-多項式 $\mathtt{Spoly1}(f_1, f_2) = 0$ であることからそれら自体の集合 $\{f_1, f_2\}$ である。しかしながら，イデアル $\langle f_1, f_2 \rangle$ の元として次のような多項式を作ることができる。

$$f_3 = a \cdot f_1 - f_2 = ax - 1。$$

f_3 は f_1 と f_2 を割ることより，$\{f_3\}$ も $\langle f_1, f_2 \rangle$ のグレブナ基底である。明らかに，$\{f_3\}$ は $\{f_1, f_2\}$ よりも表現として簡単である。**しかしながら，$\{f_3\}$ はアルゴリズム FirstGB では計算することができない。**

3.2 第 2 の計算方法（ブロック項順序を用いる方法）

ここでは，FirstGB とは違うグレブナ基底計算アルゴリズムを見る。この方法は，$K[\bar{A}][\bar{X}]$ 上のイデアルを同型な環 $K[\bar{A}, \bar{X}]$ 上のイデアルと見ることで，$K[\bar{A}, \bar{X}]$ 上でグレブナ基底を計算することである。この場合，項順序として $\bar{X} \gg \bar{A}$ となるブロック項順序を使うことで簡単に $K[\bar{A}][\bar{X}]$ のグレブナ基底を計算できることがよく知られている。まず，$K[\bar{A}, \bar{X}]$ 上の S-多項式とリダクションを **Spoly1** と **Reduce1** を区別するために **Spoly2** と **Reduce2** と書くことにする。すなわち，$f, g \in K[\bar{A}, \bar{X}]$ をゼロでない多項式としたとき $\mathtt{Spoly2}(f, g) = \frac{\mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))}{\mathrm{lm}(f)} f - \frac{\mathrm{lcm}(\mathrm{lpp}(f), \mathrm{lpp}(g))}{\mathrm{lm}(g)} g$ とし，$f = a\alpha + f_1, g = b\alpha\beta + g_1$ で $\mathrm{lm}(f) = a\alpha \in K[\bar{A}, \bar{X}]$, $a, b \in K$, $\alpha, \beta \in \mathrm{pp}(\bar{A}, \bar{X})$ とし $f_1, g_1 \in K[\bar{A}, \bar{X}]$ だとすると，その時，"$g \xrightarrow{f}_{r2}$" は $g \xrightarrow{f}_{r2} b\alpha\beta + g_1 - ba^{-1}\beta(a\alpha + f_1)$ である。ここで $b\alpha\beta$ は g の先頭単項で有る必要はない。また，多項式の集合 F でのリダクションは自然に定義され $\xrightarrow{F}_{r2}$ と書くことにする。参照 [BW93, Win96]。

アルゴリズム 2 SecondGB($F, \succ$) (Gröbner basis with Block)
Input: F: $K[\bar{A}][\bar{X}]$ の有限部分集合，$\succ$: $\mathrm{pp}(\bar{X})$ の項順序，
Output G: $\succ$ に関する $\langle F \rangle$ のグレブナ基底。

1. 集合 F を $K[\bar{A},\bar{X}]$ 上の集合と見る。
2. ブロック項順序 $\succ_{\bar{X},\bar{A}}:=(\succ,\succ_1)$ に関しての $\langle F\rangle$ のグレブナ基底 G を $K[\bar{A},\bar{X}]$ で計算する。ここで、$\succ_1$ は $\mathrm{pp}(\bar{A})$ の任意の項順序である。
3. 集合 G を $K[\bar{A}][\bar{X}]$ 上の集合と見る。その時，G は $K[\bar{A}][\bar{X}]$ 上で $\succ$ に関して $\langle F\rangle$ のグレブナ基底である。

このアルゴリズムにおいて特別な S-多項式 **Spoly1** とリダクション **Reduce1** は必要ないので，このアルゴリズムは FirstGB より効率的な計算方法だと考えられる。しかしながら，このアルゴリズムには次のような問題がある。

問題 2
$\mathbb{Q}[a,b][x,y,z]$ の多項式の集合として $F=\{f_1=ax+1, f_2=(b+1)y, f_3=az+bz+z\}$ を考える。今，$\succ$ を $\mathrm{pp}(x,y,z)$ 上の辞書式順序で $x\succ y\succ z$ とする。アルゴリズム SecondGB よりまず F を $\mathbb{Q}[a,b,x,y,z]$ の集合として考える。次に，ブロック項順序 $\succ_{\{x,y,z\},\{a,b\}}=(\succ,\succ_{glex})$ よりグレブナ基底を $\mathbb{Q}[a,b,x,y,z]$ 上で計算する。ここで，$\succ_{glex}$ を全次数辞書式順序とし $a\succ_{glex} b$ とする。その時，$\mathbb{Q}[a,b,x,y,z]$ 上のブロック項順序 $\succ_{\{x,y,z\},\{a,b\}}$ に関して $\langle F\rangle$ のグレブナ基底は

$$G=\{g_1=(a+b+1)z, g_2=(b+1)y, g_3=yz, g_4=ax+1, g_5=(b+1)xz-z\}$$

である。G は $\mathbb{Q}[a,b,x,y,z]$ 上 $\succ_{\{x,y,z\},\{a,b\}}$ に関して簡約グレブナ基底なので $g\in G$ は $G\backslash\{g\}$ によって簡約されない。しかしながら，g_5 を見ると $\mathbb{Q}[a,b][x,y,z]$ 上で $\mathrm{lm}_{\{x,y,z\}}(g_5)\in\langle \mathrm{lm}_{\{x,y,z\}}(G\backslash\{g_5\})\rangle$ である。つまり，g_5 は $\mathbb{Q}[a,b][x,y,z]$ 上では以下のように書かれる。

$$g_5=x\cdot g_1-z\cdot g_4$$

すなわち，g_5 は $\mathbb{Q}[a,b][x,y,z]$ 上では，g_1 と g_4 によってゼロに簡約される。g_5 は冗長な多項式であることが分かる。**しかし，$G\backslash\{g_5\}$ はアルゴリズム SecondGB によっては計算されない。**

4 簡約グレブナ基底

本章では，多項式環を係数ドメインとする多項式環上での簡約グレブナ基底を定義しその計算アルゴリズムを与える。まず，第 1 と第 2 の計算方法から予想される簡約グレブナ基底について述べる。この簡約グレブナ基底を弱簡約グレブナ基底として次で定義する。

定義 5 (弱簡約グレブナ基底)
$\succ_{\bar{X},\bar{A}}:=(\succ_{\bar{X}},\succ_{\bar{A}})$ をブロック項順序とし，I を $K[\bar{A}][\bar{X}]$ 上のイデアルとする。そのとき，$\succ_{\bar{X}}$ と $\succ_{\bar{A}}$ における I の**弱簡約グレブナ基底**とは，I の $\succ_{\bar{X}}$ における $K[\bar{A}][\bar{X}]$ 上のグレブナ基底で，各 $p\in G$ において次を満たすものである。

1. $K[\bar{A},\bar{X}]$ 上において項順序 $\succ_{\bar{X},\bar{A}}$ に関して，$\mathrm{Mono}(p)$ の全ての元は $\langle \mathrm{lm}(G\backslash\{p\})\rangle$ に属さない。
2. $K[\bar{A}][\bar{X}]$ 上において項順序 $\succ_{\bar{X}}$ に関して，$\mathrm{Mono}_{\bar{X}}(p)$ の全ての元は $\langle \mathrm{lm}_{\bar{X}}(G\backslash\{p\})\rangle$ に属さない。
3. 項順序 $\succ_{\bar{X},\bar{A}}$ に関して $\mathrm{lc}(p)=1$ である。

ここで自然な疑問として次がある。

どのようにこの弱簡約グレブナ基底を計算するか？

多項式環 $K[\bar{A}][\bar{X}]$ は多項式環 $K[\bar{A},\bar{X}]$ と同型より $K[\bar{A},\bar{X}]$ と見ることができる。この点において，弱簡約グレブナ基底を計算するために 2 つのリダクション **Reduce1** と **Reduce2**，2 つの S-多項式 **Spoly1** と **Spoly2**

を使うことができる。これらを使うことによってこの弱簡約グレブナ基底を計算することが可能になる。例えば，問題 1 においてグレブナ基底 $\{f_1 = ax^2 - a, f_2 = (a^3 - a)x - a^2 + 1\}$ を考えた。ここで，もし **Reduce2** もしくは **Spoly2** をこのグレブナ基底に適応したら，その時 $ax - 1$ を次のようにして得ることができる。

$$f_2 \xrightarrow{f_1}_{r2} ax - 1 \text{ もしくは } \mathtt{Spoly2}(f_1, f_2) = ax - 1。$$

ここで，$\{ax - 1\}$ は弱簡約簡約グレブナ基底の定義を満たす。
問題 2 では，グレブナ基底として $G = \{g_1, g_2, g_3, g_4, g_5\}$ を第 2 の計算方法より得た。ここで G にリダクション **Reduce1** を適応する。そのとき，$\mathrm{lpp}_{\{x,y,z\}}(g_1)$ と $\mathrm{lpp}_{\{x,y,z\}}(g_4)$ は $\mathrm{lpp}_{\{x,y,z\}}(g_5)$ を割り，そして $\mathrm{lc}_{\{x,y,z\}}(g_5) = -\mathrm{lc}_{\{x,y,z\}}(g_1) + \mathrm{lc}_{\{x,y,z\}}(g_4) = -(a+b+1) + a = -b - 1$ となることより，$g_5 \xrightarrow{\{g_1,g_2\}}_{r1} 0$ を得ることができる。したがって，g_5 は冗長な多項式であり **Reduce1** によって見つけられた。弱簡約グレブナ基底の定義より $\{g_1, g_2, g_3, g_4\}$ が弱簡約グレブナ基底である。

Algorithm 3 WRGB$(F, \succ_1, \succ_2)$ (Weak reduced Gröbner bases)
Input F: $K[\bar{A}][\bar{X}]$ の有限部分集合，$\succ_1$: $\mathrm{pp}(\bar{X})$ 上の項順序，
　　$\succ_2$: $\mathrm{pp}(\bar{A})$ 上の項順序，$(\succ_{\bar{X},\bar{A}} := (\succ_1, \succ_2)$: $\mathrm{pp}(\bar{A}, \bar{X})$ 上のブロック項順序,)
Output G: $\langle F \rangle$ の $\succ_1$ と $\succ_2$ に関する弱簡約グレブナ基底。
begin
　$G \leftarrow$ FirstGB もしくは SecondGB で $\langle F \rangle$ のグレブナ基底の計算; $E1 \leftarrow 0$
 while $E1 \neq 1$ **do**
　if $\exists p \in G$ s.t. $\left(p \xrightarrow{\{G\backslash\{p\}\}}_{r1} p_1\right)$ or $\left(p \xrightarrow{\{G\backslash\{p\}\}}_{r2} p_1\right)$ **then**
　　if $p_1 \neq 0$ **then** $G \leftarrow \{G\backslash\{p\}\} \cup \{p_1\}$ **else if** $G \leftarrow G\backslash\{p\}$ **end-if**
　else-if $E1 \leftarrow 1$
　end-if
 end-while
return(G)
end
定理 6
アルゴリズム WRGB は終了し，出力は弱簡約グレブナ基底である。

$K[\bar{A}]$ は Noether 環であるので，$K[\bar{A}][\bar{X}]$ も Noether 環である。イデアルの昇鎖列は停止することと，各リダクションを考えることより簡単に停止性と出力は弱簡約グレブナ基底になることは証明される。(証明略)

アルゴリズム 3 WRGB において，もしアルゴリズム FirstGB をグレブナ基底の計算のために適応したならば，その時 syzygy 計算 **Spoly1** と拡張グレブナ基底アルゴリズム [BW93]"**Reduce1**" が必要となる。一般的に，syzygy 計算と拡張グレブナ基底アルゴリズムの計算量，時間は大である。しかしながら，アルゴリズム SecondGB を適応すればこれらの計算は不要であるので FirstGB を適応するよりも効率的である。実際，SecondGB は一般的な体を係数とする多項式環上のグレブナ基底計算であるので，多くの計算機代数システムにすでに実装されている。現在，高速なグレブナ基底計算プログラムを持つものとして計算機代数システム **Singular**，**Risa/Asir**，**Magma** がよく知られている。簡約グレブナ基底を計算するとき，または実装するときにこれらのプログラムを使うことでより効率的に計算できる。

次に簡約グレブナ基底の性質について述べる。今ここで，一般的ドメインの簡約グレブナ基底としての一般的性質，**"唯一性" を $K[\bar{X}][\bar{A}]$ 上の弱簡約グレブナ基底は満たすか？**と言う疑問がある。この答えは**「満たさない！」**である。$K[\bar{A}][\bar{X}]$ 上のあるイデアルが与えられ，項順序が固定されたとき弱簡約グレブナ基底は唯一に決められない。次の簡単な例を見る。

例 2
$F=\{(ab+1)xy,(ac+1)xy\}$ を $\mathbb{Q}[a,b,c][x,y]$ の部分集合とし，$\succ_{\{x,y\},\{a,b,c\}}=(\succ_{lex},\succ_{lex})$ を $x\succ_{lex}y$，$a\succ_{lex}b\succ_{lex}c$ を持つブロック項順序とする。ここで，$\succ_{lex}$ は辞書式順序である。このとき，$\mathbb{Q}[a,b,c][x,y]$ 上で F はそれ自身が $\langle F\rangle$ の弱簡約グレブナ基底である。ここで，$\langle F\rangle=\langle(ac+1)xy,(b-c)xy\rangle$ となることを簡単に言うことができる。このとき，$\{(ac+1)xy,(b-c)xy\}$ もまた $\langle F\rangle$ の弱簡約グレブナ基底でことが定義より簡単に言うことができる。したがって，弱簡約グレブナ基底は与えられたイデアルと項順序に対して唯一には決められないことが分かる。

上の例で弱簡約グレブナ基底は唯一の形を持たないことがわかった。これはなぜか？この原因は係数の制約が弱いところにある。定義 5 の性質 3 では係数を 1 としている。しかしながら，考えている係数ドメインは多項式環なのでその多項式環上でもう少し強い制約がなければ $K[\bar{A}][\bar{X}]$ 上での弱簡約グレブナ基底は唯一には定まらない。この制約を考慮に入れた簡約グレブナ基底が次の強簡約グレブナ基底である。この強簡約グレブナ基底を定義するために，係数を制約するために次の 2 つを定義する。

定義 7
$\mathrm{pp}(\bar{A})$ 上の項順序を固定し，F を $K[\bar{A}]$ の部分集合とし I を $K[\bar{A}]$ のイデアルとする。イデアル I に関する F の**正規形**とは，F を I のグレブナ基底で割ったゼロでないすべての余りの集合のことである。

集合 $G\subset K[\bar{A}]$ が剰余環 $K[\bar{A}]/I$ 上でのイデアル $\langle F\rangle$ の**簡約グレブナ基底**であるとは，イデアル I に関する $\langle F\rangle$ の $K[\bar{A}]$ 上での簡約グレブナ基底の正規形のことを呼ぶ。

注意 1
グレブナ基底計算アルゴリズムと割り算アルゴリズム (レダクション) はよく知られている。この $K[\bar{A}]/I$ 上で簡約グレブナ基底は計算可能である。また，この簡約グレブナ基底は与えられた F と項順序によって唯一に決められる。

次に，弱簡約グレブナ基底より厳格な簡約グレブナ基底を定義する。この簡約グレブナ基底を**強簡約グレブナ基底**と呼ぶようにする。

定義 8 (強簡約グレブナ基底)
I を $K[\bar{A}][\bar{X}]$ のイデアルとし，$\succ_{\bar{X},\bar{A}}:=(\succ_{\bar{X}},\succ_{\bar{A}})$ をブロック項順序，G を $K[\bar{A}][\bar{X}]$ の部分集合とする。各 $e\in\mathrm{lpp}_{\bar{X}}(G)$ において，$G_e=\{f\,|\,\mathrm{lpp}_{\bar{X}}(f)=e\}$ とする。そのとき，項順序 $\succ_{\bar{X}}$ と $\succ_{\bar{A}}$ に関しての I の**強簡約グレブナ基底** G とは，$K[\bar{A}][\bar{X}]$ 上で I の $\succ_{\bar{X}}$ に関するグレブナ基底であり，各 $p\in G$ で次を満たすものである。

1. $K[\bar{A},\bar{X}]$ 上において項順序 $\succ_{\bar{X},\bar{A}}$ に関して，$\mathrm{Mono}(p)$ の全ての元は $\langle\mathrm{lm}(G\backslash\{p\})\rangle$ に属さない。
2. $K[\bar{A}][\bar{X}]$ 上において項順序 $\succ_{\bar{X}}$ に関して，$\mathrm{Mono}_{\bar{X}}(p)$ の全ての元は $\langle\mathrm{lm}_{\bar{X}}(G\backslash\{p\})\rangle$ に属さない。
3. 各 $e\in\mathrm{lpp}_{\bar{X}}(G)$ において，J_e を $F=\{\mathrm{lc}_{\bar{X}}(g)|g\in G\backslash G_e\ s.t.\ \mathrm{lpp}_{\bar{X}}(g)|e\}$ によって生成されたイデアルとする。このとき，$\mathrm{lc}_{\bar{X}}(G_e)$ は剰余環 $K[\bar{A}]/J_e$ 上で $\succ_{\bar{A}}$ に関してそれ自身が簡約グレブナ基底である。(もし $F=\emptyset$ なら，$K[\bar{A}]/J_e=K[\bar{A}]$ とする。)

問題 1 をにおいて強簡約グレブナ基底を考えてみる。この問題では，グレブナ基底としてアルゴリズム FirstGB によって $G=\{f_1=a^2x-a,f_2=(a^3-a)x-a^2+1\}$ を得た。ここで，G は定義 8 の性質 3 を満たさない。先頭項の集合は $\mathrm{lpp}_{\{x\}}(G)=\{x\}$ なので，$G_x:=\{f_1,f_2\}$ と $\mathrm{lc}_{\{x\}}(G_x):=\{a^2,a^3-a\}$ となる。ここで，$K[\bar{A}]$ 上で $\langle\mathrm{lc}_{\bar{X}}(G_x)\rangle$ の簡約グレブナ基底は $\{a\}$ であるので G は強簡約グレブナ基底ではない。しかしながら，強簡約グレブナ基底を構成することができる。$\langle a\rangle=\langle\mathrm{lc}_{\{x\}}(G_x)\rangle$ なので，a は $a=c_1\,\mathrm{lc}_{\{x\}}(f_1)+c_2\,\mathrm{lc}_{\{x\}}(f_2)$ と書くことができる。ここで，$c_1,c_2\in\mathbb{Q}[a]$ で，実際，$c_1=a,c_2=-1$ であ

る。今，新しい多項式 g として $\langle g\rangle = \langle G\rangle$，$\langle \mathrm{lm}_{\{x\}}(g)\rangle = \langle \mathrm{lm}_{\{x\}}(G)\rangle$，そして $\{\mathrm{lc}_{\{x\}}(g)\}$ が $\langle \mathrm{lc}_{\{x\}}(G_x)\rangle$ の簡約グレブナ基底となるようなものを構成できる。i.e.,$g = c_1 f_1 + c_2 f_2 = af_1 - f_2 = ax - 1$ である。したがって，g は強簡約グレブナ基底である。

次のアルゴリズムによって $K[\bar{A}][\bar{X}]$ 上の強簡約グレブナ基底を計算することができる。

Algorithm 4 SRGB($F, \succ_1, \succ_2$) (Strong reduced Gröbner bases)
Input F: $K[\bar{A}][\bar{X}]$ の有限集合，$\succ_1$: $\mathrm{pp}(\bar{X})$ 上の項順序，
　　$\succ_2$: $\mathrm{pp}(\bar{A})$ 上の項順序，($\succ_{\bar{X},\bar{A}} := (\succ_1, \succ_2)$: ブロック項順序,)
Output L: 項順序 $\succ_1$，$\succ_2$ に関する $\langle F\rangle$ の強簡約グレブナ基底
begin
$G \leftarrow \langle F\rangle$ のグレブナ基底の計算; $B \leftarrow \mathrm{lpp}_{\bar{X}}(G)$; $L \leftarrow \emptyset$
 while $B \neq \emptyset$ **do** $\succ_1$ に関して B から最少項 p の選択; $B \leftarrow B \backslash \{p\}$
　$G_p \leftarrow \{f \in F \mid \mathrm{lpp}_{\bar{X}}(f) = p\}$; $G \leftarrow G \backslash G_p$; $J_p \leftarrow \{\mathrm{lc}_{\bar{X}}(f) \mid f \in G \text{ s.t } \mathrm{lpp}_{\bar{X}}(f) | p\}$
　 if $K[\bar{A}]/\langle J_p\rangle$ 上で $\mathrm{lc}_{\bar{X}}(G_p)$ は $\succ_2$ に関して簡約グレブナ基底では **"ない"then**
　$Q \leftarrow \langle Q\rangle = \langle G_p\rangle, \langle \mathrm{lm}_{\bar{X}}(Q)\rangle = \langle \mathrm{lm}_{\bar{X}}(G_p)\rangle$，そして $K[\bar{A}]/\langle J_p\rangle$ 上で $\mathrm{lc}_{\bar{X}}(Q)$ は $\succ_2$ に関して $\langle \mathrm{lc}_{\bar{X}}(G_p)\rangle$ の簡約グレブナ基底となる Q を計算
　　$L \leftarrow L \cup \{Q \downarrow_L\}$　(下を見ろ (*))
　　else-if $L \leftarrow L \cup \{G_p \downarrow_L\}$
　　end-if
 end-while
　return(L)
end
(*) $Q \downarrow_L :=$ **begin** $S \leftarrow \emptyset$
　　while $Q \neq \emptyset$ **do** Q から q を選ぶ; $Q \leftarrow Q \backslash \{q\}$; $q_1 \leftarrow (q \xrightarrow[r1 \text{ or } r2]{L})$
　　 if $q_1 \neq 0$ **then** $S \leftarrow S \cup \{q_1\}$ **end-if**
　　end-while return(S) **end**

このアルゴリズムの停止性と出力においていつも強簡約グレブナ基底であることはアルゴリズム WRGB 同様に簡単に証明される。

強簡約グレブナ基底は次のような良い性質をもつ。

定理 9
$\mathrm{pp}(\bar{X})$ 上の項順序を $\succ_1$，$\mathrm{pp}(\bar{A})$ 上の項順序を $\succ_2$ とする。ある $K[\bar{A}][\bar{X}]$ 上のイデアル I が与えられたとき，I は唯一の強簡約グレブナ基底を持つ。

この証明は体を係数とするような多項式環での簡約グレブナ基底の唯一性の証明方法と同様に，主変数 $\bar{X}$ に関しての各先頭単項の唯一性を証明し，Noether 環上のイデアルの昇鎖列は停止することを利用すれば (簡単ではないが) 証明することができる。ここではこの定理の証明は省略する。

実際，ここで定義された強簡約グレブナ基底は，[Pau92] において定義が紹介された係数ドメインが単項イデアル整域とする多項式環上での簡約グレブナ基底を含み，この場合の一般化ともなっている。

5　計算例

アルゴリズム FirstGB，SecondGB，WRGB (SecondGB を持つ) は $K = \mathbb{Q}$ の場合に計算機代数システム Risa/Asir に実装されている。ここでは，2つの例を見る。ここで使った計算機は PC[CPU: Pentium M 1.73 GHZ, OS: Windows XP] である。

例 3

a,b,x,y,z を変数とし $F=\{bxz+ay+a, y+by+3, ay^2z+bz+b, ay+a\}\subset \mathbb{Q}[a,b][x,y,z]$ とする。 ここで全次数辞書式順序で $x\succ y\succ z$ を考える。$\mathbb{Q}[a,b][x,y,z]$ 上の $\langle F\rangle$ のグレブナ基底を 3 つのアルゴリズム FirstGB, SecondGB, WRGB で計算する。

1. FirstGB によって次のグレブナ基底を得る。

```
[(b-2)*a,(a+b)*z+b,(b+1)*y+3,b*x]
(cputime: 0.07851sec)
```

   5 個の多項式を持つ。

2. SecondGB によって次のグレブナ基底を得る。

```
[(b-2)*a,(a+b)*z+b,(-b^2+2*b)*z-b^2+2*b,(b+1)*y+3,a*y+a,b*x,
 a*x,(z+1)*y+(-b+3)*z-b+3,(y+3)*x]
(cputime: 0sec)
```

   8 個の多項式を持つ。

3. WRGB によって次の弱簡約グレブナ基底を得る。

```
[(b-2)*a,(a+b)*z+b,(b+1)*y+3,b*x]
(cputime: 0.01563sec)
```

   5 個の多項式を持つ。この集合は FirstGB によって得られた多項式の集合と同じである。実際，この集合は強簡約グレブナ基底でもある。

例 4

a,b,x,y,z を変数とし $F=\{ax^2z+ay+a, axz+b, (a+1)xz+ab\}\subset \mathbb{Q}[a,b][x,y,z]$ とする。 ここで辞書式順序 $x\succ y\succ z$ を考える。$\mathbb{Q}[a,b][x,y,z]$ 上の $\langle F\rangle$ のグレブナ基底を 3 つのアルゴリズム FirstGB, SecondGB, WRGB で計算する。

1. FirstGB によって次のグレブナ基底を得る。

```
[b*a^2-b*a-b,-b*x+a*y+a,(a+1)*z*x+b*a,a*z*x+b, a*z*y+a*z+b^2*a-b^2,
(-a^3+a^2+a)*y-a^3+a^2+a]
(cputime: 0.04688sec)
```

   6 個の多項式を持つ。

2. SecondGB によって次のグレブナ基底を得る。

```
[-b*a^2+b*a+b,(a^3-a^2-a)*y+a^3-a^2-a,b*z*y+b*z-b^3*a+2*b^3,
 a*z*y+a*z+b^2*a-b^2,-b*x+a*y+a,-z*x-b*a+b]
(cputime: 0sec)
```

   6 個の多項式を持つ。

3. WRGB によって次の弱簡約グレブナ基底を得る。

```
[-b*a^2+b*a+b,(a^3-a^2-a)*y+a^3-a^2-a,a*z*y+a*z+b^2*a-b^2,
 -b*x+a*y+a,-z*x-b*a+b]
(cputime: 0.01563sec)
```

5 個の多項式を持つ。実際，この集合は強簡約グレブナ基底でもある。

6 まとめ

今まで存在した係数ドメインを多項式環とする多項式環上のグレブナ基底計算アルゴリズムでは簡約グレブナ基底は計算できないこと紹介した。また，その多項式環上での簡約グレブナ基底として弱・強簡約グレブナ基底を定義しそれらを求めるアルゴリズムを構築した。ここで強簡約グレブナ基底は与えられた項順序とイデアルによって唯一決められることが言える。

本稿で述べられたことの応用としては包括的グレブナ基底計算 [Wei92, Mon02, SS06] での分枝を減らすテクニックとして使うことができる。これにより，より良い包括的グレブナ基底を得ることができる。

参 考 文 献

[AL94] William W. Adams and Philippe Loustaunau. *An Introduction to Gröbner Bases.* AMS-Providence, 1994.

[Buc65] Bruno Buchberger. Ein Algorithmus zum Auffinden der Basiselemente des Restklassenrings nach einem nulldimensionalen Polynomideal. *Ph.D. Thesis*, 1965. Universität Innsbruck, Austria.

[BW93] Thomas Becker and Volker Weispfenning. *Gröbner Bases, a computational Approach to Commutative Algebra.* Springer New York, 1993.

[IP98] Mariano Insa and Franz Pauer. Gröbner Bases in Rings of Differential Operators. In Bruno Buchberger and Franz Winkler, editors, *Gröbner Bases and Applications*, pages 367–380. Cambridge University Press, 1998.

[KRK88] Abdelilah Kandri-Rody and Deepak Kapur. Computing a Gröbner basis of a polynomial ideal over a euclidean domain. *Journal of Symbolic Computation*, 6:37–57, 1988.

[Möl88] H. Michael Möller. On the construction of Gröbner bases using syzygies. *Journal of symbolic computation*, 6:345–359, 1988.

[Mon02] Antonio Montes. A new algorithm for discussing Gröbner basis with parameters. *Journal of Symbolic Computation*, 33/1-2:183–208, 2002.

[NG94] George Nakos and Nikolaos Glinos. Computing Gröbner Bases over the integers. *The Mathematica Journal*, 4-3:70–75, 1994.

[Pau92] Franz Pauer. On lucky ideals for Gröbner Basis Computations. *Journal of Symbolic Computation*, 14:471–482, 1992.

[SS06] Akira Suzuki and Yosuke Sato. A Simple Algorithm to compute Comprehensive Gröbner Bases using Gröbner bases. In *International Symposium on Symbolic and Algebraic Computation*, pages 326–331, 2006.

[Sti87] Sabine Stifter. A generalization of reduction rings. *Journal of Symbolic Computation*, 4(3):351–364, 1987.

[Tri78] Wolfgang Trinks. Über B. Buchbergers Verfahren, Systeme algebraischern Gleichungen zu lösen. *Journal of Number Theory*, 10:475–488, 1978.

[Wei87] Volker Weispfenning. Gröbner bases for polynomial ideals over commutative regular rings. In James H. Davenport, editor, *EUROCAL '87, LNCS378*, pages 336–347. Springer, 1987.

[Wei92] Volker Weispfenning. Comprehensive Gröbner bases. *Journal of Symbolic Computation*, 14/1:1–29, 1992.

[Win96] Franz Winkler. *Polynomial Algorithms in Computer Algebra.* Springer-Verlag Wien New York, 1996.